On Enhancing Intersection Applications With Misbehavior Detection and Mitigation

Jiahao Zhang, Ziyi Liu, Ines Ben Jemaa, Francesca Bassi, Fawzi Nashashibi

On Enhancing Intersection Applications With Misbehavior Detection and Mitigation

Jiahao Zhang*†, Ziyi Liu*, Ines Ben Jemaa*, Francesca Bassi*, Fawzi Nashashibi†
*IRT SystemX, †INRIA, France
{jiahao.zhang, ziyi.liu, ines.ben-jemaa, francesca.bassi}@irt-systemx.fr, fawzi.nashashibi@inria.fr

***Abstract*—Collective Perception Services (CPS) enable communicating entities to share their perception data in the V2X communication network. Potential attacks on extended perception data affect the CPS and may consequently degrade the safety application that rely on collective perception data. In this paper, we build an architecture that allows the integration of misbehavior detection and mitigation mechanisms with the CPS. We implement the Intersection Movement Assist (IMA) application that uses the extended perception data to calculate potential collision risks in intersection areas. We define specific safety metrics and through extensive simulations in large scale scenarios, we quantify the impact of a large number of attacks and of misbehavior detection on the safety application. Our evaluation demonstrates the ability of misbehavior detection and mitigation mechanisms to filter malicious shard perception data and consequently the benefits of using such mechanisms in improving the robustness of the safety application in complex road scenarios.**

***Index Terms*— C-ITS, Misbehavior Detection, Simulation, Collective Perception**

I. Introduction

Collective perception has achieved significant progress recently with the emergence of novel perception technologies and V2X communication capabilities. Collective Perception Services (CPS) primarily aim to overcome the limitations of individual vehicular perception in complex environments characterized by occlusions and limited sensor's field of view. Intersections are a typical example of such environments where an important number of accidents may occur. For instance, in 2019 in France 18% of fatal accidents occurred in intersection. Using collaborative perception may increase the awareness of a given vehicle about the non directly perceived objects in the intersection thanks to the V2X CAM [1] and CPM [2] messages. The information collected continuously by the collaborative perception service is greatly useful for the safety applications such as the Intersection Movement Assist (IMA) application [3]. In this application, an ego vehicle continuously evaluates the potential crash zones in the intersection by comparing its trajectory with those of other dynamic objects (e.g., vehicles, pedestrians, etc.). When an estimated risk indicator reaches a certain threshold, the application generates a local alert which is intended for instance to change the driving manoeuvre of the ego.

The IMA application relies mainly on the extended perception which is a data structure that contains the kinematic description of each known object. This data structure is obtained and updated continuously by fusing the local perception data and the V2X received messages. While fusion of perception data is a challenging process due to some factors such as data uncertainty, ambiguity or imprecision [4], it is even more challenging when there are potential attackers among the V2X transmitters. We call these attackers *misbehaving nodes*. *Misbehaving nodes* are defined according to [5] as "any node that transmits erroneous data that it should not transmit when the hardware and software are behaving as expected". More precisely, in our work, we assume that misbehaving entities are entities, which, while leveraging the shared information through V2X, send erroneous perception information to disrupt the safety applications. Misbehavior detection was studied in the last decade. First approaches rely on data plausibility and consistency verification [6]. Recently, some work address misbehavior detection on V2X perception data and use advanced techniques such as probabilistic approaches [7] or trust based approaches [8]. Validation and evaluation of misbehavior detection performance relies on usual metrics derived from false positive rate, false negative rate or other detection time related metrics. In this work, we assess the performance of misbehavior detection through its ability to overcome the impact of several types of attacks on a safety application for intersection scenarios. We first build a framework where we tightly integrate misbehavior detection and mitigation techniques to the CPS. Additionally, we implement the IMA as a proof of concept of a safety application that uses extended perception data and connect it to the simulation environment. We define metrics to assess the impact of misbehavior detection and mitigation on safety application. Through extensive simulations on large scale intersection scenarios, we demonstrate the positive effect of our misbehavior detection and mitigation module on making safety application more robust and resilient to attacks.

The rest of this paper is organized as follows: Section II presents the related work. Section III outlines our simulation framework architecture. Section IV details the simulation parameters and evaluation metrics. Section V presents the experimental results. Finally, Section VI concludes the paper.

II. Related Work

Collective perception can compensate for the shortcomings of the ego's perception when occlusions occur, and is achieved either by the exchange of raw sensor data or of processed data

[9], [10]. Many works elaborate a detailed analysis on the potential benefits of using collective perception in enhancing cooperative awareness and consequently the traffic safety.

[11] presents a highway simulation study that evaluates the benefits of using collective perception in enhancing the road safety level. The author define a set of metrics such as the Object Awareness Ratio, the Risk Awareness Ratio and the Object Tracking Accuracy. The overall results show a positive impact in increasing safety when at least 25% of participant are equipped with CPM transmission capabilities.

[12] shows the potential of sharing raw perception data through Road Side Units (RSU) and its ability to support safe passing through intersections. The study focuses on deriving the required sensor data rate to prevent collisions at intersections by evaluating the necessary braking distances under several velocity and data rates settings. [13] quantifies the occlusion risk in intersection areas with the presence of Vulnerable Road Users (VRU). The work defines the Maximum Tracking Loss metric as a safety metric that captures the period in which vehicles are not aware about VRUs in the intersection. The authors demonstrate that with a penetration rate of 25%, they are able to decrease the occlusion risk and enhance the awareness about existing VRU in the intersection.

All these works highlight the benefits of using CPS and generally V2X services for better road safety. However, several types of perturbations may limit their benefits. These perturbations may be caused by the degradation of the network performance. For instance, channel congestion and its trade-off with information freshness is one major challenge that has been identified early on [14], [15]). Other types of perturbation may be caused by the existence of attackers among the V2X communication participants. The authors of [16] investigate the impact of network attacks using the CAM messages on the network performance level. In their study, they use usual performance metrics such as the Packet Delivery Ratio to assess specific safety metrics such as the Safety Risk Index. Compared to network attacks, our work focuses on V2X data attacks which may impact semantically the safety risk assessment. [17] evaluates the impact of attacks on CAM and CPM messages on highway merging scenarios. They show the impact of both the fake arrival attacks on the highway insertion time and the mean speed, and the ghost object attack on increasing the potential accident risk. Compared to the already cited works, our work uses similar safety metrics and tailor them to the intersection scenarios. We use these metrics to quantify the impact of a large number of CPS data attacks on safety applications. We quantify also the benefits of using detection and mitigation techniques in limiting the negative impacts of the evaluated attacks on safety application.

III. General Architecture

Fig.1 presents the architecture of the platform used for evaluation in this work. The misbehavior detection and mitigation modules are tightly integrated to the global data fusion module, which produces the extended perception used by the IMA module. Due to space limitation, this section does not detail the cooperative perception architecture. Examples of such architectures may be found in [18] and [7].

A. Attack Injection

To assess the impact of the attacks on the IMA, we address several types of attacks on CPS. Basic to moderate attacks consist on changing the kinematic information of the transmitted perceived objects in the CPM message. Advanced attacks consist on creating non-existing objects (i.e. Ghost injection) or omitting existing ones (i.e. object omission). Table I summarizes the different categories of the attacks, their severity rating, the potential detection techniques and examples of the potential causes.

B. Global Data Fusion

1) Misbehavior Detection: Each received CPM and CAM message is decoded and processed by the misbehavior detection module, which verifies the message content before relaying it to the *Local perception and V2X message fusion*. We implement verification on several data levels as follows.

- Data plausibility verification: Check whether the single attributes of the perceived objects in a received CPM are plausible or not. The verification is specifically focusing on comparing the attributes with pre-defined thresholds (signal-based) or known relations to other attributes (model-based).
- Data consistency verification: Consistency verification check if the received data in the actual CPM from one source are consistent with the past received data from the same source in a certain period of time. In this verification we use kinematic rules or filtering approaches such as Kalman Filtering.
- Local perception data redundancy verification: Redundancy verification are based on the verification of V2X perception data coming from neighbors and the *Ego* local perception data. The solution is based on comparing the objects that are detected in the perception area of the *Ego* and the content of the CPM message. Due to the limitation of this approaches in occlusion scenarios, we deploy this verification only on Road Side Units with sensors that are much less impacted by occlusions in urban scenarios.

2) Misbehavior Mitigation: Misbehavior mitigation is an essential step to robustly transmit a reliable Extended Perception data to the IMA. The objective is to take the appropriate decisions when an attack on the V2X data is detected. The mitigation measures are listed below.

- Filtering the received V2X messages: The first mitigation strategy is to avoid propagating the attack in the extended perception data base. When a misbehavior is detected on a given message, the message is discarded and the V2X generating source is inserted in a blacklist structure. All the successive messages received from the same source are ignored
- Generating a Misbehavior Report: Once a misbehavior is detected, a vehicle should send an alert known as

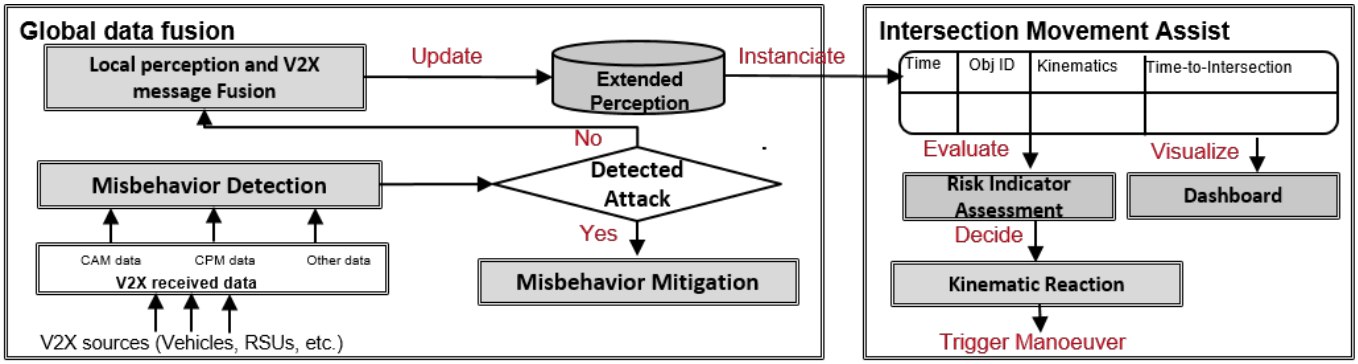

Fig. 1: The General Architecture of the integrated Misbehavior Detection and the IMA application

TABLE I: Addressed attacks

Attacks	Severity of the attack	Detection techniques	Description	Potential cause or objective
Non-plausible kinematic data	Basic	Physical law plausibility checks	The attacker sends implausible kinematic data of a perceived object such a random position	Lidar perception degrades when the perceived object is localized far from the sensor
Non-consistent kinematic data	basic/moderate	Model based consistency checks	The attacker sends inconsistent kinematic data of a perceived object in successive CPMs. For example, it sends a first CPM with a correct position and speed and a second CPM with a very high speed	Attacker simulates a sudden stop of a perceived vehicle in the road
Omission attack	moderate/advanced	Data redundancy checks	The attacker omits the existence of one or several real perceived objects in successive CPMs	Generate potential dangerous manoeuvre at the intersection
Ghost injection attack	moderate/advanced	Data redundancy checks	The attacker sends a fake perceived object with plausible and consistent kinematic data	Gain turning priority at the intersection

Misbehavior Report [19] to a back-end security server called the *Misbehavior Authority*. This report should contain the set of evidence (i.e., proof) confirming the results of the misbehavior detection. Notice that this mitigation step is out of the scope of this work.

3) Local Perception and V2X message Fusion: The local perception consists first on collecting and merging data generated from several local sensors such as Lidars, cameras, radars and etc. The main operations in this module consist on multi-sensor data fusion, which generates as an output a list of local perceived objects. Each object has a local identifier and is characterized by a set of kinematic attributes in the local reference of the *Ego* vehicle. Second, the local perception is merged with the received V2X messages to elaborate an extended view of the perceived objects in the environment. Potentially, other data may be used such as geographic maps or contextual information. As shown in Fig. 1, this module updates the **Extended Perception** which contains the list of the extended perceived objects. Each perceived object is described by a unique identifier and a set of kinematic attributes.

C. The Intersection Movement Assist Application

1) Risk Indicator Assessment: In this section, we describe the risk assessment method used by the IMA in intersection areas. For each given *Ego* vehicle equipped with V2X communication capabilities, the IMA accesses periodically the extended perception content. The access frequency is much associated to the type of the application. The more the safety decision is critical, the higher the frequency should be to ensure the freshness of the extended perception data. In our case, we set this frequency to 300 ms. We are interested in assessing the collision risk at each time t as long as a given *Ego* vehicle approaches an intersection i during its journey. A journey here is defined as the path between a starting source position and a final destination position. The IMA locates the *Ego* vehicle in the geographic map. If the *Ego* is driving towards a close intersection, the IMA calculates its *Time-To-Intersection (TTI)*. The $TTI_{v,t}$ is function of the distance $D_{v,t}$ of a given vehicle v to the center of the intersection and its velocity $V_{v,t}$ at a given time t. For each dynamic object O in the extended perception list driving towards the same intersection as the *Ego*, the IMA calculates its $TTI_{O,t}$ and the resulting difference with the *ego*, $TTI_{ego,O,t}$. The intersection collision risk in our case is an exponential function of the $TTI_{ego,O,t}$. Notice that other more complex risk assessment functions are possible [20]. We choose a simple function in our work because our focus is on studying the impact of the attacks on the IMA, as a proof Of Concept of a safety application for intersection scenarios. We may tune the risk assessment threshold by choosing more conservative values.

$$\begin{aligned} TTI_{v,t} &= \frac{D_{v,t}}{V_{v,t}} \\ TTI_{ego,O,t} &= TTI_{ego,t} - TTI_{O,t} \\ r_t &= e^{-TTI_{ego,O,t}} \end{aligned} \tag{1}$$

2) Kinematic Reaction: When a the $TTI_{Ego,i}$ reaches a certain threshold and the $r_{i,O,t}$ is higher than a certain threshold, a collision alert event is generated and displayed on the dashboard to warn the driver. Additionally, a kinematic reaction is decided and is associated to a risk severity. In

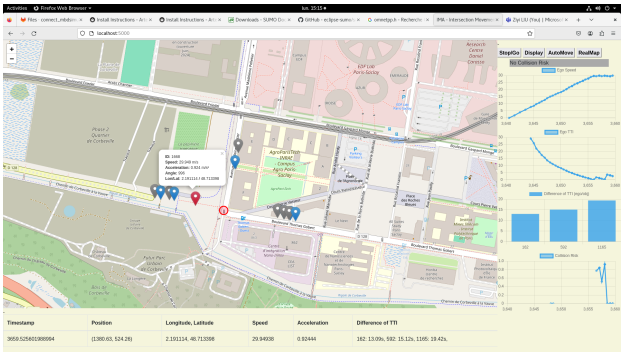

Fig. 2: Intersection Movement Assist implemented dashboard

this paper, we define two possible kinematic decisions, either stopping the vehicle through a braking manoeuvre for a certain duration of time or authorizing it to cross safely the intersection. Finally, the highest collision risk $r_{max,t}$ is selected among all the objects and displayed on the dashboard. Fig.2 shows the implemented dashboard on the IMA.

Algorithm 1 Intersection Risk Assessment

Input: Extended Perception at time t_k

Output: Risk assessment $r_{i,t}$ locate *Ego*'s current road and next close intersection i

1: calculate *Ego*'s current road and next intersection i
2: **for** each perceived object O in the extended perception list **do**
3: locate object's current road and next close intersection
4: **if** *Ego* and O are not in the same road and go towards the same intersection i **then**
5: calculate TTI difference as
6:

$$TTI_{Ego,O,i} = TTI_{Ego,i} - TTI_{O,i} r_t = e^{-TTI_{ego,obj,t}} \quad (2)$$

7: **if** $TTI_{Ego,i} \leq TTI_{threshold}$ & $r_{i,O,t} \geq r_{threshold}$ **then**
8: generate and display Collision Alert
9: brake *Ego* for a certain duration
10: **end if**
11: **end if**
12: **end for**
display $r_{max,t} = e^{min(-TTI_{ego,O,t})}$ on Dashboard

IV. Experimental Evaluation

A. Experimental Settings

We provide our simulation framework as an open source simulation platform [21]. The platform combines the Artery simulator with the CARLA simulator and the external intersection assistance application. We evaluate the IMA application under attack scenarios on a large scale. We consider the Paris Saclay network to validate our simulation framework, as shown in Fig. 3. This scenario contains a network size of 1.24 km^2 with a stable vehicle density of 18.2 vehicles/km^2. We use randomly generated vehicle traces as the test benchmark. Two levels (20% and 80%) of generated vehicles are equipped with the V2X service. We test three attacker densities with the same simulation seed. All simulation settings are shown in TABLE II.

Fig. 3: Paris Saclay Network

TABLE II: Simulation Parameters

Simulation duration	1h
Penetration rate	0.8 0.2
Total generated connected vehicles	425 87
Attacker density	0.25 0.15 0.05
Scenario size	1.24 km^2
Vehicle density	18.2 Veh / km^2
Communication media	802.11p
Communication profile	ITS-G5
Communication type	Single Hop Broadcast
CPM interval	1 sec (fixed rate)
Front radar sensor	FoV range = 200m
	FoV angle = ±20°

B. Attack Model

We consider the internal attacks in our V2X attack model. The attacker possesses a legitimate digital certificate, allowing authentication and ensuring the integrity of transmitted messages. We assume that the attacker has full priority access to sensor data and can modify sensor measurements when encoding them in the CPM. All tested attack types are depicted as follows:

- Addition of a ghost perceived object: Adding a ghost object at a random fixed position around the attacker in CPMs. All kinematic data keeps the same as the attacker.
- Omission of the perceived object:
  1) Omission of all perceived objects
  2) Omission of one specific perceived object
- Alteration on the perceived object position
  1) Random position: For each transmitted CPM, the position is chosen with uniform distribution as a random point in the map (The range is the map size).
  $Position_x = U(Map\_X_{min}, Map\_X_{max})$
  $Position_y = U(Map\_Y_{min}, Map\_Y_{max})$
  2) Constant position: The position is a fixed value within the reasonable ego's perception range.

$Const_x = U(0, max\_SensorRange_x)$
$Const_y = U(0, max\_SensorRange_y)$
$Position_x = Const_x$
$Position_y = Const_y$

3) Random position offset: For each transmitted CPM, add a noise to the actual distance data. The noise is obtained sampling from a gaussian distribution with $\mu = 0$ and $\sigma = \frac{max\_SensorRange}{10}$.
$Position_x = current\_Position_x + N(0, \frac{max\_SensorRange}{10})$
$Position_y = current\_Position_y + N(0, \frac{max\_SensorRange}{10})$

- Alteration on the speed

1) Random speed: For each transmitted CPM, the speed is chosen from a uniform distribution.
$Speed_x = U(0, Max\_Speed)$
$Speed_y = U(0, Max\_Speed)$
2) Constant speed: The speed is a fixed value within the max reasonable speed.
$Const_x = U(0, Max\_Speed)$
$Const_y = U(0, Max\_Speed)$
$Speed_x = Const_x$
$Speed_y = Const_y$
3) Random speed offset: For each transmitted CPM, add a noise to the actual speed data. The noise is obtained sampling from a gaussian distribution with $\mu = 0$ and $\sigma = \frac{current\_Speed}{10}$.
$Speed = current\_Speed + N(0, \frac{current\_Speed}{10})$

C. Evaluation Metrics

We define a set of metrics to evaluate the impact of attacks and misbehaviour detection and remediation in a large-scale simulation setting. In order to allow comparison, we run the same Paris Saclay Network scenario, with fixed vehicle trajectories, for the following cases:

(i) Genuine nominal condition (i.e., no attack)
(ii) Attack condition, for different types of attacks with different severity levels
(iii) Attack condition with MBD, for the same attacks of the previous situation, when misbehavior detection and mitigation measures deployed in each *Ego* vehicle

The metrics that we compare for each of the previous situations are the following:

a) Average Intersection Awareness: The Intersection Awareness of the ego vehicle is a function describing the number of objects in its extended perception w.r.t the distance from the intersection center as it approaches the intersection. In a large scale scenario, the Average Intersection Awareness (AIA) is the cumulative Intersection Awareness of the ego, considered over all the intersections in the scenario, and averaged by the number of vehicles in the simulation. Similarly to the Environment Awareness Ratio presented in [11], this metric captures the awareness of the ego, with the difference that we concentrate on the intersection area. The AIA is chosen as an indicator to evaluate the impact of attacks: it increases when the attack has the capability of fabricating non-existent objects; it decreases when the effect of the attack is the masking of information.

b) Total Collision Alert Events: As described in Section III-C, a Collision Alert Event (CAE) is raised by the IMA application when an assessed risk reaches a certain threshold. On the large scale scenario, we evaluate the cumulative number of CAE (raised by all vehicles during the entire simulation). Comparing the Total Collision Alert Events in the three situations described above allows to assess the number of missed collision alerts and the number of false collision alerts generated by the application. Notice that a collision alert usually leads to a braking manoeuvre and has a significant safety impact on the traffic scenario.

c) Average Waiting Time: The Waiting Time is defined as the cumulative time that a vehicle spends at a standstill throughout the entire simulation. The Average Waiting Time is the average across all vehicles in the simulated scenario. It's interesting to look at this metric since the reaction of the IMA application to an alert is to stop the ego vehicle. Hence, the Average Waiting Time is going to positively correlate with the Total CAE. Examining the increase of the Average Waiting Time in case of attacks allows to provide an indication of the impact of the attacks on traffic congestion.

V. Discussion

A. Average Intersection Awareness (AIA)

Fig. 4 shows the AIA for the simulation of the Paris Saclay Network, for the different types of attacks, with a penetration rate 0.8 and attacker rate of 0.25. We compare the nominal condition (green) with the attack condition (red), and we find that the DropAllObj, the DropObj attacks have an impact on the AIA, decreasing the awareness of the ego. On the other hand, the AddObj, SigleConstDist, SingleRandomDist attacks increase the AIA of the ego: notice that this is due to the fact that the ego now perceives either non-existent objects, or perceives the same object more than once.

Finally, we consider the impact of misbehavior detection and mitigation (blue). In general, for the nominal case, the AIA with the misbehaviour detection is slightly lower than that of the nominal case due to occasional false positives from the misbehavior detection system. For the DropAllObj and DropObj attacks, misbehavior detection obviously does not bring an improvement in the AIA since the information was missing in the first place. However, in the case of position alteration attacks, we can see that the misbehavior detection and mitigation system is able to bring the AIA back very close to the nominal values.

B. Total Collision Alert Events

Table III presents the Total Collision Alert Events for the Paris Saclay Network under different penetration rates in presence of the considered attacks. In the genuine case, the Total CAE is 694 when the penetration rate is 0.8, and 164 when the penetration rate is 0.2. The Table presents the variation of the Total CAE with respect to the Total CAE in the nominal case. In Table III we show the impact that

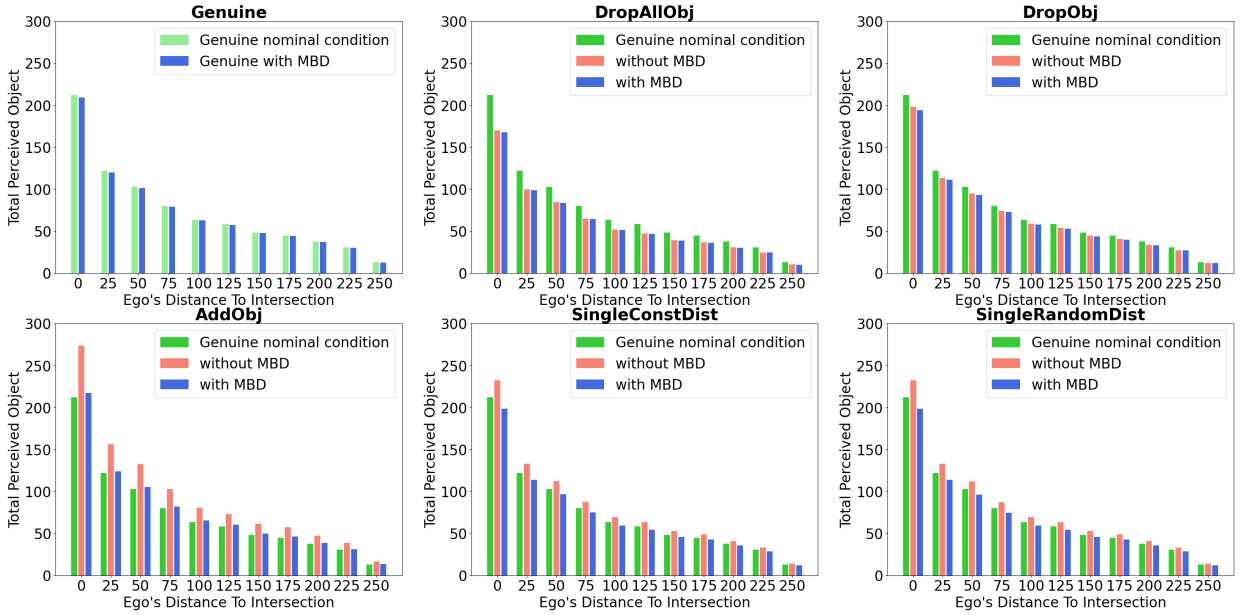

Fig. 4: Average Intersection Awareness. The Intersection Awareness describes the number of objects in the extended perception of the ego, as a function of their distance from the intersection; the average is with respect to all vehicles in the simulation.

TABLE III: Total Collision Alert Events with different CPS penetration rates

Attack Type	**Total Collision Alert Events** (Penetration Rate 0.8)		**Total Collision Alert Events** (Penetration Rate 0.2)	
	Without MBD	**With MBD**	**Without MBD**	**With MBD**
AddObj	1019 (+46.83%)	818 (+17.86%)	165 (+0.61%)	165 (+0.61%)
DropAllObj	685 (-1.29%)	684 (-1.44%)	165 (+0.61%)	165 (+0.61%)
DropObj	707 (+1.87%)	705 (+1.585%)	165 (+0.61%)	166 (+1.22%)
SingleConstDisOffset	694 (+0%)	694 (+0%)	164 (+0%)	164 (+0%)
SingleConstDis	718 (+3.46%)	696 (+0.288%)	165 (+0.61%)	165 (+0.61%)
SingleConstSpeedOffset	715 (+3.03%)	699 (+0.72%)	165 (+0.61%)	166 (+1.22%)
SingleConstSpeed	729 (+5.04%)	696 (+0.288%)	165 (+0.61%)	165 (+0.61%)
SingleRandomDisOffset	862 (+24.21%)	711 (+2.45%)	166 (+1.22%)	165 (+0.61%)
SingleRandomDis	698 (+0.58%)	696 (+0.288%)	165 (+0.61%)	165 (+0.61%)
SingleRandomSpeedOffset	700 (+0.865%)	695 (+0.144%)	164 (+0%)	165 (+0.61%)
SingleRandomSpeed	729 (+5.04%)	696 (+0.288%)	165 (+0.61%)	165 (+0.61%)

TABLE IV: Total Collision Alert Events with different attacker rates

Attack Type	**Total Collision Alert Events** (Attacker Rate 0.25)		**Total Collision Alert Events** (Attacker Rate 0.15)		**Total Collision Alert Events** (Attacker Rate 0.05)	
	Without MBD	**With MBD**	**Without MBD**	**With MBD**	**Without MBD**	**With MBD**
AddObj	1019 (+46.83%)	818 (+17.86%)	912 (+31.41%)	796 (+14.70%)	743 (+7.06%)	717 (+3.31%)
DropAllObj	685 (-1.30%)	684 (-1.44%)	701 (+1.01%)	701 (+1.01%)	696 (+0.288%)	696 (+0.288%)
DropObj	707 (+1.87%)	705 (+1.59%)	700 (+0.86%)	697 (+0.43%)	695 (+0.144%)	695 (+0.144%)

each attack type has on the CAE. When the penetration rate is low (0.2), the attacks have a negligible impact, since almost all the CAE events are triggered on information based on the vehicle's local perception. When the penetration rate is high (0.8) it is clearly visible that the attacks AddObj and SingleRandomDistOffset have the biggest impact, increasing the Total CAE by 46.83% and 24.21%, respectively compared to the genuine scenario. This is due to the fact that these attacks trigger the addition of non existent objects to the extended perception; this observations are coherent with what observed with respect to the variation of the AIA metric.

We can see that when the misbehaviour detection and mitigation is in place the impact of these attacks is highly mitigated: for the SingleRandomDistOffset attack the Total CAE is brougth back nearly at the same level as the genuine case (only 2.5% increase); also for the AddObj we observe that the excess number of alerts is greatly reduced, although not quite back to the nominal case (18% excess with respect to the nominal case still remaining).

In Table IV we focus on the impact of varying the attacker rate, for a selected subset of attacks and for penetration rate 0.8. As expected, for the AddObj attack, the attacker rate is proportional to the number of Total CAE events. The misbehaviour detection and mitigation measures help in reducing the excess alerts. For the DropAllObj and DropObj attacks, we remark the possibly counter-intuitive result that the presence of the attack does not seem to impact the Total CAE. This is explained by the fact that in a high penetration scenario,

thanks to the redundancy of the available information, most of the time the ego still manages to achieve awareness of the surrounding objects, even in presence of an attacker in the neighborhood.

C. Average Waiting Time

We considered the Average Waiting Time for the Paris Saclay Network, for penetration rate 0.8. The Average Waiting Time for the genuine case is of 15.796 seconds. We then consider the case of AddObj attack without misbehavior detection, with a rate of 0.25, and find an increase in the Average Waiting Time of 13.51%, i.e., 17.93 seconds. In the case of AddObj with misbehavior detection, we find an improvement in the Average Waiting Time of 6.7%, i.e., 16.87 seconds.

D. Limitations in the current contribution

We tested our framework on only one generated traffic set; future work includes repeating the study on different traffic sets, involving more vehicles.

Other than on the total number of vehicles, the total number of generated collision alerts highly depends on the parameters chosen for the attack. Depending on these, more missed alerts or false alerts may be generated as a consequence of the same attack event. In future work we plan to study the sensitivity of our results with respect to those parameters.

We also conducted simulations with different simulation seeds. With different seeds, there were some missed collision alerts for certain types of attacks, which we did not include in this paper. However, with misbehavior detection, the collision alert can be refined, approaching the genuine condition.

VI. CONCLUSION

In this paper, we present an enhanced intersection application framework. We show that the integration of misbehavior detection into CPS significantly enhances the reliability and safety of intersection applications by effectively mitigating the adverse effects of V2X data manipulation attacks. Our proposed approach demonstrates significant potential in increasing the robustness of safety applications in intersection scenarios. For future work, we plan to update framework by integrating advanced misbehavior detection solutions based on trust mechanisms. Additionally, we plan to test our framework in multiple traffic scenarios.

ACKNOWLEDGMENT

This research work has been carried out in the framework of the Technological Research Institute SystemX, and has received funding from the European Union's Horizon 2020 EU Research & Innovation program under Grant Agreement No 101069688 (H2020-EU CONNECT).

REFERENCES

[1] ETSI TS 103 900 V2.0.0 (2022-07), "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Specification of Cooperative Awareness Basic Service; Release 2," Standard, Jul. 2022.

[2] ETSI TS 103 324 V2.1.1 (2023-06), "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Collective Perception Service; Release 2," Standard, Jun. 2023.

[3] 5GAA, "C-v2x use cases and service level requirements," 5GAA Automotive Association, Tech. Rep., 2023.

[4] B. Khaleghi, A. Khamis, F. O. Karray, and S. N. Razavi, "Multisensor data fusion: A review of the state-of-the-art," *Information Fusion*, p. 28–44, jan 2013. [Online]. Available: https://doi.org/10.1016/j.inffus.2011.08.001

[5] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Communications Surveys Tutorials*, 2019.

[6] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE Transactions on Vehicular Technology*, 2020.

[7] C. Allig, T. Leinmüller, P. Mittal, and G. Wanielik, "Trustworthiness estimation of entities within collective perception," in *2019 IEEE Vehicular Networking Conference (VNC)*.

[8] J. Zhang, I. B. Jemaa, and F. Nashashibi, "Trust management framework for misbehavior detection in collective perception services," in *2022 17th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, 2022.

[9] A. Caillot, S. Ouerghi, P. Vasseur, R. Boutteau, and Y. Dupuis, "Survey on cooperative perception in an automotive context," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 14 204–14 223, 2022.

[10] X. Gao, X. Zhang, Y. Lu, Y. Huang, L. Yang, Y. Xiong, and P. Liu, "A survey of collaborative perception in intelligent vehicles at intersections," *IEEE Transactions on Intelligent Vehicles*, 2024.

[11] F. A. Schiegg, I. Llatser, D. Bischoff, and G. Volk, "Collective perception: A safety perspective," *Sensors (Basel, Switzerland)*, vol. 21, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:229942735

[12] R. Fukatsu and K. Sakaguchi, "Automated driving with cooperative perception using millimeter-wave v2v communications for safe overtaking," *Sensors (Basel, Switzerland)*, vol. 21, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:233396011

[13] V. A. Wolff and E. Xhoxhi, "Mitigating vulnerable road users occlusion risk via collective perception: An empirical analysis," 2024.

[14] S. Joerer, B. Bloessl, M. Segata, C. Sommer, R. L. Cigno, and F. Dressler, "Fairness kills safety: A comparative study for intersection assistance applications," in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*. IEEE, 2014, pp. 1442–1447.

[15] T. Zinchenko, H. Tchouankem, and L. Wolf, "Reliability of vehicle-to-vehicle communication at urban intersections," in *2014 7th International Workshop on Communication Technologies for Vehicles (Nets4Cars-Fall)*. IEEE, 2014, pp. 7–11.

[16] Z. Pethő, Z. Szalay, and Árpád Török, "Safety risk focused analysis of v2v communication especially considering cyberattack sensitive network performance and vehicle dynamics factors," *Vehicular Communications*, vol. 37, p. 100514, 2022.

[17] M. Hadded, P. Merdrignac, S. Duhamel, and O. Shagdar, "Security attacks impact for collective perception based roadside assistance: A study of a highway on-ramp merging case," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2020, pp. 1284–1289.

[18] M. Ambrosin, L. L. Yang, X. Liu, M. R. Sastry, and I. J. Alvarez, "Design of a misbehavior detection system for objects based shared perception v2x applications," in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*. IEEE, 2019, pp. 1165–1172.

[19] ETSI TS 103 759 V2.1.1 (2023-01), "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2," Standard, Jan. 2023.

[20] S. G. McGill, G. Rosman, T. Ort, A. Pierson, I. Gilitschenski, B. Araki, L. Fletcher, S. Karaman, D. Rus, and J. J. Leonard, "Probabilistic risk metrics for navigating occluded intersections," *IEEE Robotics and Automation Letters*, vol. 4, no. 4, 2019.

[21] J. Zhang, I. B. Jemaa, and F. Nashashibi, "Simulation Framework of Misbehavior Detection and Mitigation for Collective Perception Services," in *35th IEEE Intelligent Vehicles Symposium (IV 2024)*, Jeju Island, South Korea, Jun. 2024.